UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,016	05/10/2006	Vesa Torvinen	P18450US1	1254

27045 7590 07/21/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
BENOIT, ESTHER	

ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
07/21/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

Office Action Summary	Application No.	Applicant(s)	
	10/595,016	TORVINEN ET AL.	
	Examiner	Art Unit	
	ESTHER BENOIT	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-14,16-20 and 22-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-14,16-20 and 22-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Action is in response to a Pre-Appeal brief request made on April 8, 2010. Claims 1-3, 5-14, 16-20, and 22-33 are pending in this application. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

Response to Arguments

2. Applicant's arguments, see Remarks, filed 4/8/2010, have been fully considered. Some arguments are found persuasive and some are not. Therefore, the rejection has been withdrawn. The arguments that are not found persuasive are addressed below. Upon further consideration, a new ground(s) of rejection is made in view of Inoue et al. (US 2006/0034238 A1).

Arguments under 35 U.S.C. 103 (a)

***Arguments to Claim 1*:**

a) Niemi does not disclose "generating a password based on the HTTP Digest Challenge is associated with the identity of the remote server and the identity of the end-user as created by the remote server"

Response to arguments of Claim 1:

As to point a: The argument has been considered but is not persuasive. On page 10, point 3, Niemi discloses a response sent from the server to the client that requested

access, includes realm data which is data associated with the remote server the user is requesting access to and User ID generated for the remote server the client wants to gain access to. Therefore, Niemi's password is generated based on the remote server's identity.

As to any claims not specifically discussed, the applicants argued that it was patentable for one of the reasons discussed above. Please see response to above arguments for unspecified discussions.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3,5-14,16-20 and 22-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over of Reiche (6,092,196), in view of Niemi et al. (RFC 3310, HTTP Digest Authentication Using AKA), and further in view of Inoue et al. (US 2006/0034238 A1).

With respect to claims 18, Reiche discloses:

- receiving a request for access from said UE by said remote server (Col. 8, lines 47-49, *customer server receives request from client to access a URL on the customer server*);

- creating the temporary identity for the UE by said remote server (Col. 8, lines 64-67, *Authentication Daemon inside of customer server detects client is not authenticated and further creates unique client ID for client*);
- sending to an authentication node, details of the request for access, said details including said temporary identity created by said remote server (Col. 9, lines 6-26, *AD in customer server redirects client's browser to authentication server for authenticating the client. AD passes URL string and transaction ID to authentication server, wherein URL string includes client ID*).
- at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the temporary identity of the UE created by said remote server (Col. 9, lines 15-32, *401 authentication challenge is sent back to client's browser causing authentication server to redirect control to user's browser for password input*);
- storing the password and the temporary identity of the UE at the UE (Col. 9, lines 30-31, *where client's browser retains authentication information*);
- receiving a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server (Col. 9, lines 27-37, *client is able to input authentication data received from authentication server in dialog window to show proof that user ID and password have been obtained*).

Reiche does not explicitly disclose authentication node to generate a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user password with details of temporary identity of the UE and identity of the remote server;

However, Niemi discloses authentication node to generate a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user password with details of temporary identity of the UE and identity of the remote server (pg. 10, point 3) "Request containing credentials", *where realm is the remote server identity and username is the identity of the UE. The user is being authenticated to gain access to mobile.biz server*);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche with the teachings of Niemi to generate an HTTP Digest challenge including identity of the remote server and the temporary identity of the UE, *because* it will allow the user secure access to the server and recall the credentials for accessing that remote server at a later period.

Reiche and Niemi do not explicitly disclose the authentication node can also reside in the UE's home network.

However, Inoue discloses the authentication node can also reside in the UE's home network ([0092]-[0098], *registration request is received at Home Agent along with password and user ID to check if user is legitimate or not*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche and Niemi with the

teachings of Inoue to include an authentication node in the home network, *because* it will allow the user secure access to its home network when roaming on a visited network.

With respect to claim 1, the limitations of claim 1 are similar to the limitations as claim 18. Therefore, the claim is rejected for the same reasons as claim 18 above. Please see rejection above.

With respect to claims 2 and 19, Reiche does not explicitly disclose the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA)

However, Niemi discloses the method, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA) (pg. 6, paragraph 2, "If the server…", and pg. 7, paragraph 1, "When a client…")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche with the teachings of Niemi to use HTTP Digest Authentication and Key Agreement, *because* it will allow for better password encryption.

With respect to claim 3, Reiche discloses sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server and wherein the identity of the remote server is stored at the UE (Col. 9, lines 6-26, *AD in customer server redirects client's browser to authentication server for authenticating the client. AD passes URL string and transaction ID to authentication server, wherein URL string*

includes client ID and Col. 9, lines 30-31, *where client's browser retains authentication information*);

With respect to claims 5 and 22, Reiche discloses sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node (Col. 4, lines 50-67 and Col. 5, lines 1-17, *where the user request for access is redirected to an authentication server*)

With respect to claims 6 and 23, Reiche discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE (Col. 9, lines 15-32, *401 authentication challenge is sent back to client's browser causing authentication server to redirect control to user's browser for password input*);

With respect to claims 7 and 24, Reiche discloses the method, wherein the password is stored at the authentication node (Col. 12, lines 61-63)

With respect to claims 8 and 25, Reiche discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated (Col. 9, lines 37-67)

With respect to claims 9 and 26, Reiche discloses sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly (Col. 5, lines 12-31, *where the user request for access is redirected to an authentication server*)

With respect to claims 10 and 27, Reiche discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the

remote server (Col. 9, lines 15-26, *customer browser remote from authentication server*)

With respect to claims 11 and 28, Reiche discloses the method, wherein the HTTP Digest challenge is generated at the remote server (Col. 9, lines 15-26, *customer browser remote from authentication server*)

With respect to claims 12 and 29, Reiche discloses the method, further comprising sending the HTTP digest challenge from the remote server to the UE (Col. 9, lines 15-26, *customer browser remote from authentication server*)

With respect to claims 13 and 30, Reiche discloses authenticating the UE at the remote server (Col. 9, lines 22-36)

Reiche does not explicitly disclose a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server.

However, Niemi discloses HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server (pg. 6, paragraph 2, “If the server…", and pg. 7, paragraph 1, “When a client…”)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche with the teachings of Niemi to use HTTP Digest Authentication and Key Agreement, *because* it will allow for better password encryption.

With respect to claims 14 and 31, Reiche discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (Col. 9, lines 38-67)

With respect to claim 16, Reiche discloses sending an authentication request from the remote server to the authentication node, (Col. 5, lines 12-43) sending the password from the authentication node to the remote server, (Col. 5, lines 54-67) and authenticating the UE at the remote server (Col. 9, lines 22-36).

With respect to claim 17, Reiche discloses sending an authentication request from the remote server to the authentication node, (Col. 9, lines 6-26) authenticating the UE at the authentication node (Col. 9, lines 37-67) and sending confirmation of authentication from the authentication node to the remote server (Col. 5, lines 32-42).

With respect to claim 20, Reiche does not explicitly disclose sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server and wherein the identity of the remote server is stored at the UE.

However, Niemi discloses sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server and wherein the identity of the remote server is stored at the UE (pg. 10, point 3) "Request containing credentials", *where realm is the remote server identity and username is the identity of the UE. The user is being authenticated to gain access to mobile.biz server*);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche with the teachings of Niemi to generate an HTTP Digest challenge including identity of the remote server and

the temporary identity of the UE, *because* it will allow the user secure access to the server and recall the credentials for accessing that remote server at a later period.

With respect to claims 32-33, This claim is similar to claims 1 and 18 with the exception of subsequent requests made. Therefore, the claim limitations are rejected for the same reasons as claims 1 and 18 above. In addition, Reiche discloses performing said authentication without generating any additional password and without contacting said authentication node in the home network (Col. 11, lines 25-43)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esther Benoit whose telephone number is 571-270-3807. The examiner can normally be reached on Monday through Friday between 7:30 a.m and 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Philip Lee can be reached on 571-272-3967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.B.
July 8, 2010

/Philip C Lee/
Acting SPE of Art Unit 2442